REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Claim Objections

This objection has been addressed by amending method claims 5 and 6 to depend from method claim 4, rather than from system claim 3.

2. Rejection of Claims 1-6 Under 35 USC §103(a) in view of U.S. Patent Nos. 6,023,764 (Curtis) and 6,253,248 (Nakai)

This rejection is respectfully traversed on the grounds that neither the Curtis patent nor the Nakai patent discloses or suggests, whether considered individually or in any reasonable combination, a secured-communications-establishing system in which, as claimed:

- an authentication server supplies mobile code to the user's computing device upon authenticating the user (for example, by means of a password), without requiring pre-installation of authentication and encryption client software on the user's computing device, *i.e.*, without authentication by the user's computing *device* of the server that supplies the mobile code; and
- the mobile code establishes a secured communications pathway to the application server through the authentication server, with mutual authentication between the mobile code and the authentication server (*i.e.*, the mobile code authenticates itself to the *authentication* server, and in addition authenticates the *application* server).

Instead, the system described in the Curtis patent at least requires authentication of the server by the user's computing device, and preferably requires mutual authentication between the user's computing device and the server before any mobile code can be downloaded. The system described in the Nakai patent merely converts data for use in communications between a client and application server that utilize different protocols.

Whereas the goal of the claimed invention is to eliminate the need for pre-installation of client software for each applications server by using mobile code to establish pathways to the application server from any platform, including mobile and thin client platforms, regardless of the specific authentication method (while at the same time providing authentication of the mobile code at the time the pathways are established), Curtis requires such pre-installation.

It is true that the server of Curtis supplies mobile code, but the mobile code does not have all of the features of the claimed mobile code. In particular, it does not have the self-authenticating feature. As explained on pages 5 and 6 of the "BACKGROUND" section of Applicant's specification, while the system described in the Curtis patent (U.S. Patent No. 6,023,764) utilizes mobile code in the form of Java applets to secure communications between a user's computer and an application or "web" server, it only does so following authentication of the server, which is why the system of Curtis uses **certificates *pre-installed* in the user's web browser**. Before any communications can occur, the user's web browser must verify a certificate sent by the server (**Fig. 4A of Curtis**), after which a secure socket layer (SSL) connection is established and a Java applet sent to the web browser. Only then does the Java applet of Curtis retrieves keys from the web server for use in opening a secure socket or stream to the web server.

Since the Curtis system can be implemented by any application server, Curtis is justifiably concerned with authentication of, at least, the mobile-code-supplying server (as well as the user *or* user's computer), thereby **necessitating** the pre-installation of the above-mentioned pre-installed certificates as well as corresponding software unique to each service to be accessed. In the claimed invention, on the other hand, authentication of the mobile code server is not really a problem since the server is an authentication server contacted by the user (for example one supplied by the user's ISP) and not some unknown application server. Thus, according to the claimed invention, the user can pre-register with the authentication server, permitting authentication of the user without the need to authenticate the user's computing device, and thereby enabling the user to use *any* computing device. **Requiring pre-installed certificates, as in Curtis, eliminates the principal advantage of server-based computing, which is to**

permit a registered user to access a service from any computing device using a standard communications protocol, regardless of the computing device's configuration.

On the other hand, from the point of view of a subsequently contacted application server, the system of Curtis patent has the disadvantage that it fails to provide for authentication of the mobile code itself before sending a "key certificate" to the applet containing the code, leaving the application server vulnerable to anyone capable of re-creating or copying the mobile code and requesting the key certificate for use in protecting further communications.

These deficiencies of the system disclosed in the Curtis patent are not made up for by the Nakai patent, which is directed to data conversion by a proxy server, and not to establishing secure communications using mobile code. Nakai neither discloses nor suggests:

- **modification** of Curtis' establishment of secured pathways, which requires ***authentication*** of the **application server** ***before*** downloading the mobile code from the **application server** to the user's computing device, based on ***pre-installed certificates***, by instead
- having an **authentication server** download mobile code ***without mutual authentication*** of the **user's computer** and the **authentication server**, the mutual authentication between the mobile code itself and the authentication server coming **after** download of the mobile code, the user's-computing-device to application server authentication of Curtis being replaced by arranging the mobile code to authenticate itself to the **authentication server** to which the application server is connected, as claimed.

In fact, the Nakai patent does not describe any sort of authentication or mobile code. Instead, the Nakai patent describes a way to connect a client and application server that use different communications protocols by having the proxy server perform the conversion. The use of proxy servers is of course well known, and it is certainly possible to implement Curtis' system using such a proxy server. However, the result will not be the claimed invention.

In the system of Curtis, the "client" and the application server mutually authenticate each other by means of certificates pre-installed in the client's browser and keys in the server, after which mobile code is downloaded for use in securing further communications. A possible combination of Curtis' system in view of Nakai would be to have the client and a proxy server, as taught by Nakai, mutually authenticate each other by means of certificates pre-installed in the client's browser, as taught by Curtis. However, this would still not achieve the advantages of the claimed invention, in which the *authentication* server authenticates the user by, for example, a password entered by the user, whereupon mobile code is sent to the user's computer so as to establish secured communications with the *application server*, the mobile code providing the necessary certificates to establish mutual authentication with the *authentication* server.

Although the authentication server of the claimed invention could be arranged as a "proxy server," it does not serve the same function as the proxy server of Nakai. The claimed authentication server does not convert data for facilitating communications with the client and application server using different protocols. Instead, the claimed authentication server is a mobile code supplier that supplies authentication programs for use is establishing secured communications with application servers. In other words, the authentication server of the claimed invention supplies the certificates necessary to establish the secured communications, so that the client does not need to have the certificates pre-installed. As a result, *any* client capable of receiving and executing mobile code can be used to establish secured communications with *any* application server capable of authenticating the certificates provided by the mobile code. If an application server is capable of authenticating a particular type of certificate, then the proxy server supplies the appropriate certificate, together with the appropriate code for carrying out the authentication.

The Curtis system does not have this versatility. Instead, it utilizes pre-installed certificates that can only be authenticated by servers having corresponding keys. While downloading of mobile code to establish further communications is advantageous, Curtis does not go far enough, *i.e.*, it does not enable download of the secured-communications-establishing

mobile code to any client, including mobile devices and thin computing devices, without pre-installed authentication certificates.

The Nakai patent, which does not describe any sort of authentication, much less authentication between the client and application server using mobile code downloaded by the authentication server, clearly does not suggest the proposed modification of Curtis's system to enable such download of secured-communications-establishing mobile code from an authentication server to a client computing device based solely on *user* identification without pre-installed certificates, as claimed. Therefore, withdrawal of the rejection of claims 1-6 under 35 USC §103(a) in view of the Curtis and Nakai patents is respectfully requested.

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: September 20, 2004

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500